# QGroup präsentiert »Best of Hacks«: Highlights Februar 2020

Frankfurt am Main, 03. Mai 2021 – Mit der höheren Online-Nutzung während der Corona-Pandemie steigen auch die Angriffe von Hackern im privaten Bereich, in Wirtschaft und Politik. Im Februar wurde unter anderem der Cyberangriff auf die Domain der Programmiersprache Perl publik. Zeitweise kam es zum totalen Verlust der Webseite. Auch ein Wasserwerk in Florida wurde Ziel eines Angriffs.

Die Domain Perl.com der freien, plattformunabhängigen Programmiersprache wurde von unbekannten Angreifern vollständig übernommen und gehijackt. Seither verweist die Domain auf eine IP-Adresse, die in Zusammenhang mit kriminellen Aktivitäten steht. Die Domain wurde unrechtmäßig von den Angreifern für 190.000 US-Dollar zum Verkauf angeboten. Die legitimen Besitzer der Domain haben Entwicklern, die Perl.com als Mirror zum Beziehen von Perl-Modulen via CPAN (Comprehensive Perl Archive Network) nutzen, empfohlen, die Konfiguration von CPAN.pm auf cpan.org zu ändern. Vor einem Besuch der Domain Perl.com wurde gewarnt.

Hacker haben im US-Bundesstaat Florida kurzzeitig die Kontrolle über die Trinkwasseraufbereitung des Wasserwerkes der Stadt Oldsmar übernommen. Die Einstellungen der Grundwasseraufbereitungsanlage, die die Zufuhr von Natriumhydroxid regelt, wurden manipuliert und auf das 100-fache erhöht. Ein Mitarbeiter beobachtete den Eingriff und reagierte sofort. Natriumhydroxid zersetzt in einer höheren Konzentration Gewebe. Ein Schaden für die Bevölkerung konnte so abgewendet werden.

Cyberkriminelle erlangten Zugriff auf Server von CD Projekt S.A., einem polnischen Entwickler und Publisher von Computerspielen, der unter anderem "Cyberpunk 2077" entwickelt hat. Die Angreifer erbeuteten Source Code von mehreren Projekten der Entwicklungsabteilung CDPR Red. So waren die Spiele "Cyberpunk 2077", "The Witcher 3" und die Stand-Alone-Variante des Kartenspiels "Gwent" betroffen. Die Daten, die durch die Ransomware-Attacke verschlüsselt wurden, konnten laut Aussage von CD Projekt S.A. durch Backups wiederhergestellt werden. Die Angreifer drohten auch mit der Veröffentlichung von erbeuteten Dokumenten.

Unbekannte Angreifer haben die Kunden- und Kommunikationssysteme von Netcom Kassel Gesellschaft für Telekommunikation mbH kompromittiert. Dabei wurden Kundendaten gestohlen, die dann auf einer eigenen Webseite veröffentlicht wurden, um den Provider zu erpressen.

(2.332 Zeichen)

Medienkontakt:

QGroup GmbH
Berner Straße 119
60437 Frankfurt am Main
www.qgroup.de/presse

Lars Bothe
Tel.: +49 69 17 53 63-014
E-Mail: l.bothe@qgroup.de